

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----	X	
	:	
GOOGLE LLC,	:	
	:	
Plaintiff,	:	
	:	21cv10260 (DLC)
-v-	:	
	:	<u>OPINION AND ORDER</u>
DMITRY STAROVIKOV, ALEXANDER FILIPPOV,	:	
	:	
AND DOES 1-15,	:	
	:	
Defendants.	:	
-----	X	

APPEARANCES:

For plaintiff:

Andrew Zenner Michaelson  
Kathleen Elizabeth McCarthy  
King & Spalding LLP (NYC)  
1185 Avenue of the Americas  
New York, NY 10036

Bethany Rupert  
King & Spalding  
1180 Peachtree Street NE  
Atlanta, GA 30309

David Paul Mattern  
King & Spalding LLP (DC)  
1700 Pennsylvania Avenue, N.W.  
Washington, DC 20006

For defendants:

Igor B. Litvak  
The Litvak Law Firm, PLLC  
1733 Sheepshead Bay Road  
Suite 22  
Brooklyn, NY 11235

DENISE COTE, District Judge:

Google LLC ("Google") has brought claims against defendants Dmitry Starovikov and Alexander Filippov for operating a botnet to steal and exploit Google users' personal information. The Clerk of Court entered a default against the two defendants on February 8, 2022.

Google now moves for the entry of a default judgment against the defendants. The defendants have moved to set aside the entry of default and to dismiss the case for lack of jurisdiction. For the following reasons, the defendants' motion to set aside the entry of default is granted and the other motions are denied.

### **Background**

#### **I. Factual Background**

The following facts are taken from the Complaint. Google alleges that the defendants control the Glupteba botnet. A botnet is a network of private computers infected with malware. This malware hijacks the infected computers, instructing them to execute commands issued by a command-and-control server (also called a "C2 server"), which controls the botnet. Google alleges that the defendants use the Glupteba botnet as part of a

criminal scheme (the "Glupteba Enterprise") to hijack victims' computers and steal their personal information.

Conventional botnets receive instructions from C2 servers whose domains or IP addresses are hardcoded in the botnet malware. This means that a conventional botnet can be disabled by taking the server at the hardcoded address offline. The Glupteba malware, however, instructs infected computers to look for the addresses of its C2 servers by referencing transactions associated with specific accounts on the Bitcoin blockchain. The blockchain is not controlled by any central authority, and each transaction is disseminated to and viewable by any user on the blockchain. These features make the Glupteba botnet unusually resistant to disruption. If the botnet's C2 servers are disabled, the Glupteba Enterprise can simply set up new servers and broadcast their addresses on the blockchain.

Google alleges that the defendants use the Glupteba botnet to further several unlawful schemes. First, the botnet steals Google account information from infected devices, and access to those stolen accounts is then sold to third parties. Second, the defendants sell credit cards to third parties packaged with stolen accounts. Customers then use those the credit cards to pay for Google services, but the cards do not provide full

payment when charged. Third, the botnet places disruptive ads on infected computers. Fourth, the defendants sell access to the infected devices as proxies, allowing third parties to route their internet traffic through the infected devices, disguising its origin. And fifth, the defendants hijack infected computers to mine cryptocurrency.

The Glupteba Enterprise's schemes are carried out through websites owned by a set of related corporate entities, all sharing the same address. Google alleges that the defendants have used email addresses and physical addresses associated with these entities, and that they signed up for their Google accounts using devices with the same IP addresses as the Glupteba Botnet's C2 servers.

## II. Procedural History

Google filed the present lawsuit on December 2, 2021, bringing claims for violation of the Racketeer Influenced and Corrupt Organizations ("RICO") Act, the Computer Fraud and Abuse Act ("CFAA"), the Electronic Communications Privacy Act ("ECPA"), trademark and unfair competition law, and for tortious interference with a business relationship and unjust enrichment. The complaint requests damages, attorney's fees, injunctive relief, and declaratory relief. Google also requested a

temporary restraining order enjoining the defendants from their allegedly unlawful activities, and permitting Google to request that entities providing services to domains and IP addresses associated with the Glupteba botnet take reasonable best efforts to disrupt the botnet.

A Temporary Restraining Order (the "TRO") issued on December 7, granting the requested relief. The TRO authorized Google to use alternative service "via mail, email, text, and/or service through ICANN" to serve the defendants.<sup>1</sup> The TRO also ordered the defendants to appear on December 16 to show cause why the TRO should not be converted into a preliminary injunction.

On December 8, Google served the TRO, complaint, and order to show cause on defendants. The Court held a hearing on December 16, at which the defendants did not appear. The Court then converted the TRO into a preliminary injunction. On January 31, Google reported that it had successfully disabled all of the C2 servers operating at the time the complaint was

---

<sup>1</sup> ICANN is the International Corporation for Assigned Names and Numbers, a non-profit organization responsible for managing the internet's Domain Name System and allocating IP addresses, among other duties. See "Beginner's Guide to Participating in ICANN", ICANN (Nov. 8, 2013), <https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf>.

filed, along with several more servers set up since.

Additionally, Google had shut down several domains and Google accounts associated with the Glupteba botnet.

On February 7, Google requested an entry of default against defendants Starovikov and Filippov. Google submitted with its request a declaration that Google had served the defendants by mail, email, and text message. The Clerk of Court issued a certificate of default on February 8.

On February 24, the defendants proposed a briefing schedule for an intended motion to set aside the entry of default. At a conference on March 1, a schedule was set for the defendants' motion, as well as Google's motion for default judgment. The defendants filed a motion to set aside the default and dismiss the case on March 14. Google filed a motion for default judgment on March 25, withdrawing its request for damages or attorney's fees in connection with its motion. The defendants' motion to set aside the entry of default became fully submitted on April 8, and Google's motion for entry of default judgment became fully submitted on April 15.

### **Discussion**

A court may "set aside an entry of default for good cause." Fed. R. Civ. P. 55(c). To determine whether good cause

has been shown, a court must assess three criteria: "(1) the willfulness of default, (2) the existence of any meritorious defenses, and (3) prejudice to the non-defaulting party."

Bricklayers & Allied Craftworkers Local 2, Albany, N.Y. Pension Fund v. Moulton Masonry & Constr., LLC, 779 F.3d 182, 186 (2d Cir. 2015) (citation omitted). "Other relevant equitable factors may also be considered, for instance, whether the failure to follow a rule of procedure was a mistake made in good faith and whether the entry of default would bring about a harsh or unfair result." Enron Oil Corp v. Diakuhara, 10 F.3d 90, 96 (2d Cir. 1993).

#### I. Willfulness

Willfulness "refer[s] to conduct that is more than merely negligent or careless," but is instead "'egregious and not satisfactorily explained.'" Bricklayers, 779 F.3d at 186 (quoting SEC v. McNulty, 137 F.3d 732, 738 (2d Cir. 1998)). A default may be found willful where "an attorney failed . . . for flimsy reasons to comply with scheduling orders; or failed, for untenable reasons, after defendants have purposely evaded service for months, to answer the complaint." McNulty, 137 F.3d

at 738-39 (citation omitted).<sup>2</sup> In Bricklayers, for example, the Second Circuit found that a default was willful when there was no dispute that the defendant “was aware of the legal action pending against him and his company,” but the defendant nevertheless “failed to file a responsive pleading for over nine months after the receipt of the summons and complaint, nearly eight months after the defendants were informed that the plaintiffs had requested an entry for default, and six months after they were served with discovery demands.” Id.

The date on which the defendants received actual notice of this litigation is disputed. The defendants have submitted declarations stating that they did not receive service of any papers through mail or email, and that they were unaware of this action until January of 2022, when a friend saw a news report about it and showed it to them. Filippov concedes that he may have received service through text message, but claims to have quickly deleted the message because he thought it looked suspicious. After they were alerted to the lawsuit in January, the defendants claim that they took some time to translate the

---

<sup>2</sup> Although McNulty was decided under Fed. R. Civ. P. 60(b), the Second Circuit has relied on cases involving relief from default judgment under Rule 60(b) to inform the standard to set aside an entry of default under Rule 55(c). See Bricklayers, 779 F.3d at 186 n.1; Fed. R. Civ. P. 55(c).



complaint and retain a Russian-speaking attorney in the United States. Their attorney then filed a notice of appearance on February 10, and filed a request to schedule a motion to vacate the entry of default on February 24 -- a little more than two weeks after the certificate of default was issued.

Google argues that there is abundant evidence that defendants were aware of the case sooner than they claim, because they should have received notice at least through Russian media coverage of the case, if not through many of the other methods of service. Google points to Russian-language coverage of their complaint in outlets such as BBC Russia and Novaya Gazeta. Google also notes that it attempted to serve the defendants at the address listed at their company's website, via email to their Google accounts, via notification through ICANN, via SMS text message, and through WhatsApp. Finally, Google points out that, since obtaining a TRO, Google has successfully disrupted the Glupteba botnet, taking many of its C2 servers and associated websites offline. Google argues that the defendants must be aware of this disruption, because they have scrambled to set up new C2 servers to continue this scheme.

As improbable as it may be for all of Google's attempts at service to have failed to provide the defendants with actual

notice, there remains a dispute that the defendants were aware of the legal action pending against them. Bricklayers, 779 F.3d at 187. Moreover, the defendants waited only two weeks after the entry of a default to request to move to vacate the default. On this record, the Court will not find that the defendants' delay constitutes a willful default.

## II. Meritorious Defenses

A court may decline to set aside an entry of default when the defaulting party has presented no meritorious defense. See State Street Bank & Trust Co. v. Inversiones Errazuris Limitada, 374 F.3d 158, 174 (2d Cir. 2004); Sony Corp. v. Elm State Elecs., Inc., 800 F.2d 317, 320-21 (2d Cir. 1986). To establish the existence of a meritorious defense, a defendant must present "evidence of facts that, if proven at trial, would constitute a complete defense." Green, 420 F.3d at 109 (citation omitted). Mere "conclusory denials," however, are not sufficient "to show the existence of a meritorious defense." Bricklayers, 779 F.3d at 187 (citation omitted).

The defendants assert several bases for dismissal of the complaint, including lack of personal jurisdiction, insufficient service of process, forum non conveniens, and failure to state a claim. For the reasons explained below, however, these

arguments are not meritorious, and do not justify setting aside the default.

The defendants also dispute the truth of Google's allegations. The defendants concede that they are employed by Valtron, one of the entities that Google alleges forms part of the Glupteba Enterprise. And they acknowledge that they worked on at least some of the websites that Google alleges form part of the defendants' unlawful scheme. Nevertheless, the defendants claim to lack knowledge of the criminal schemes that Google alleges they control. They assert as well that they did not intend to target U.S. users and that user participation in their services is entirely legitimate and voluntary. These declarations are sufficient to raise a question of fact that must be resolved at a later stage. Accordingly, the defendants' motion to vacate the default is granted, and Google's motion for default judgment is denied.

A. Personal Jurisdiction

The defendants argue that the Court must set aside the entry of default and dismiss the case because it lacks personal jurisdiction over them. Google disagrees and also insists that the defendants have waived any personal jurisdiction defense. "A court will obtain, through implied consent, personal

jurisdiction over a defendant if the actions of the defendant during the litigation amount to a legal submission to the jurisdiction of the court, whether voluntary or not.” Mickalis Pawn Shop, LLC, 645 F.3d at 134 (citation omitted). Google argues that the defendants consented to personal jurisdiction in an email exchange with Google’s counsel,<sup>3</sup> and during the Court’s March 1 conference. In both instances, however, the defendants’ waiver was contingent on Google withdrawing its motion for default judgment. As Google has not done so, the defendants have not waived their personal jurisdiction defense.

“To defeat a motion to dismiss for lack of personal jurisdiction, a plaintiff must make a prima facie showing that jurisdiction exists.” Charles Schwab Corp. v. Bank of Am. Corp., 883 F.3d 68, 81 (2d Cir. 2018) (citation omitted). To make such a showing, the plaintiff must allege sufficient facts to establish that there is a basis for jurisdiction under the law of the forum State, and that “the exercise of personal jurisdiction comports with due process.” Id. at 82. See also Fed. R. Civ. P. 4(k)(1)(A).

---

<sup>3</sup> Federal Rule of Evidence 408 does not prohibit consideration of the emails, because they are not offered “to prove or disprove the validity or amount of a disputed claim or to impeach by a prior inconsistent statement or contradiction.” Fed. R. Evid. 408(a).

The Due Process Clause requires that the defendant "have certain minimum contacts with the forum state such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice." Licci ex rel. Licci v. Lebanese Canadian Bank, SAL, 732 F.3d 161, 169 (2d Cir. 2013) (quoting Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945)). This analysis can be broken down into three steps. U.S. Bank Nat'l Assoc. v. Bank of Am. N.A., 916 F.3d 143, 150 (2d Cir. 2019). "First, the defendant must have purposefully availed itself of the privilege of conducting activities within the forum State or have purposefully directed its conduct into the forum State." Id. (citing J. McIntyre Machinery, Ltd. v. Nicastro, 564 U.S. 873, 877 (2011) (plurality opinion)). "Second, the plaintiff's claim must arise out of or relate to the defendant's forum conduct." Id. (citation omitted). And third, the court must determine that jurisdiction is "reasonable under the circumstances." Id. (citation omitted).

The defendants claim that Google has not demonstrated that they have minimum contacts with the State of New York, and that it would be unreasonable to bring them into court here when the Russian Federation has a more significant interest in this dispute. The defendants' argument does not succeed in showing

that the defendants have a meritorious defense regarding jurisdiction.

Google has alleged sufficient contacts between each of the defendants and the State of New York to establish personal jurisdiction under New York's long arm statute and the Due Process Clause. See N.Y. C.P.L.R. § 302(a)(3). Google has alleged that the defendants operate a botnet that has infected over one million devices, at least thousands of which are located in New York City. Additionally, Google alleges that the defendants intentionally infected devices in New York in order to steal victims' personal information. Parties who create "continuing relationships . . . with citizens of a[] state are subject to regulation and sanctions in [that] State for the consequences of their activities." Chloe v. Queen Bee of Beverly Hills, LLC, 616 F.3d 158, 172 (2d Cir. 2010) (quoting Burger King v. Rudzewicz, 471 U.S. 462, 472-73 (1985)). By allegedly infecting New York devices with malware and continuing to issue those devices commands, the defendants have established this kind of "continuing relationship."

Defendants argue that jurisdiction in New York is nevertheless inappropriate, because the defendants did not intend to target U.S. users with their software and online

services. They assert that U.S. users constitute less than 1% of all users. But the geographic breadth of the defendants' activities in general "does not diminish any purposeful contacts" with New York victims in particular. See id. at 171. This is particularly true where, as here, the defendants are alleged to have committed "an intentional tort," which may bring the defendants "within the State's authority by reason of [their] attempt to obstruct its laws." J. McIntyre Machinery, Ltd., 564 U.S. at 880 (plurality opinion).

The defendants also argue that jurisdiction is not reasonable under the circumstances, because Russia has a greater interest in adjudicating the case, and because it would be "literally impossible" for the defendants to appear in court in the United States. The defendants have not explained Russia's interest in hearing the case, however, except to point out that the defendants are Russian residents. But a defendants' residence in another country does not preclude the exercise of personal jurisdiction, even when the plaintiffs have not alleged injury within the United States. See Licci, 732 F.3d at 173-74. Here, Google has alleged that the defendants have infected and hijacked devices within New York. Additionally, the "conveniences of modern communication and transportation ease

any burden the defense of this case in New York might impose” on the defendants. Id. at 174. And the defendants have not shown that they would be unable to reach the United States if necessary by flying through a country over which Russian air traffic is not banned.<sup>4</sup> The defendants have therefore failed to show that personal jurisdiction is unreasonable under the circumstances.

B. Insufficient Service of Process

The defendants argue that the default must be vacated and the case against them dismissed because they were not properly served. An individual in a foreign country may be served by any “means not prohibited by international agreement, as the court orders.” Fed. R. Civ. P. 4(f)(3). Additionally, under the Due Process Clause, service must be “reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections.” Oneida Indian Nation

---

<sup>4</sup> See, e.g., Heileng Tan, Business Insider, “Emirates Says It Will Continue Flying to Russia as Long As the Dubai Government Tells it To, Weeks After Major Airlines Suspended Operations to the Country” (Mar. 30, 2022, 1:46 AM), <https://www.businessinsider.com/emirates-airline-russia-flights-dubai-government-ukraine-war-2022-3>.



of N.Y. v. Madison County, 665 F.3d 408, 428 (2d Cir. 2011) (quoting Jones v. Flowers, 547 U.S. 220, 226 (2006)).

On December 7, 2021, Google was ordered to serve the defendants "via mail, email, text, and/or service through ICANN." The defendants do not deny that Google attempted service through these methods, among others. Nor do the defendants argue that these methods of service were prohibited by international agreement.

Instead, the defendants claim simply not to have received service. But "actual notice" is not required, only means "reasonable calculated" to achieve it. See id. Google's attempts to serve the defendants easily satisfy this standard. When a defendant's address is known, service by mail is sufficient to satisfy due process. Id. at 429. And when mail is impracticable, notice by publication may be sufficient. See Brody v. Village of Port Chester, 434 F.3d 121, 129 (2d Cir. 2005). Here, Google not only attempted to serve the defendants by mail at the address located on their company's website, Google also served the defendants via text message, email, WhatsApp message, and by other means. Moreover, Filippov's declaration indicates that he likely received service through

text message. The defendants therefore have no meritorious defense for insufficient service of process.

C. Forum non Conveniens

The defendants argue that the default should be set aside and the case dismissed pursuant to the doctrine of forum non conveniens. The doctrine of forum non conveniens does not provide the defendants with a meritorious defense that would support removal of a default. In any event, the defendant's invocation of the doctrine fails on the merits.

"The principle of forum non conveniens is simply that a court may resist imposition upon its jurisdiction even when jurisdiction is authorized by the letter of a general venue statute." Norex Petroleum Ltd. v. Access Indus., Inc., 416 F.3d 146, 153 (2d Cir. 2005) (quoting Gulf Oil Corp. v. Gilbert, 330 U.S. 501, 507 (1947)). When analyzing a motion to dismiss due to forum non conveniens, a district court must "(1) determine the degree of deference properly accorded to the plaintiff's choice of forum; (2) consider whether the alternative forum proposed by the defendants is adequate to adjudicate the parties' dispute, and (3) balance the private and public interests implicated in the choice of forum." Aenergy, S.A. v.

Republic of Angola, 2022 WL 1099445, at \*4 (2d Cir. Apr. 13, 2022).

The decision to dismiss under forum non conveniens lies “wholly within the broad discretion of the District Court.” Id. (citation omitted). Nevertheless, “[a] defendant invoking forum non conveniens ordinarily bears a heavy burden in opposing the plaintiff’s chosen forum.” Sinochem Int’l Co. Ltd. v. Malaysia Int’l Shipping Corp., 549 U.S. 422, 430 (2007).

1. Degree of Deference

Forum non conveniens dismissal is not warranted here. First, a plaintiff’s choice of forum is “generally entitled to great deference when the plaintiff has sued in the plaintiff’s home forum.” Iragorri v. United Tech. Corp., 274 F.3d 65, 71 (2d Cir. 2001). And this deference is “even stronger when the plaintiff is an American citizen and the alternative forum is a foreign one.” Olympic Corp. v. Societe Generale, 462 F.2d 376, 378 (2d Cir. 1972). Google is a United States corporation, and has sued in United States District Court. Google’s choice of a forum within the United States therefore deserves significant deference.

2. Adequacy of the Alternative Forum

Second, the defendants have not shown that Russia provides an appropriate alternative forum. "An alterative forum is adequate [1] if the defendants are amenable to service of process there, and [2] if it permits litigation of the subject matter in dispute." Anergy, S.A., 2022 WL 1099445, at \*5 (citation omitted). The defendants have not demonstrated that they are amenable to service of process in Russia -- and their emphatic protests that they never received service despite Google's many attempts suggest otherwise. Nor have the defendants "represent[ed] that they would all submit to the jurisdiction of Russian courts in any comparable action filed against them by the plaintiff." Norex Petroleum Ltd., 416 F.3d at 157.

Additionally, the defendants have not shown that Russian courts would permit litigation of the subject matter in dispute. They have submitted no expert opinions or other evidence to support that Russian courts are functioning and would be adequate forums to litigate the conduct at issue here, including in a case with an American corporation and Russian defendants. The defendants point to Russia's intellectual property law, which suggests that Russian courts might be amenable to litigate

Google's trademark claims. But the defendants do not address any other conduct underlying the complaint. Accordingly, they have not satisfied their burden to show that an adequate alternative forum exists.

### 3. Public and Private Interest

Because the defendants have not demonstrated the existence of an alternative forum, dismissal on the grounds of forum non conveniens "must be denied" regardless of any other factors. Norex, 416 F.3d at 157. Nevertheless, a balancing of the public and private interest factors also weighs against dismissal.

A case should only be dismissed on the grounds of forum non conveniens "if the chosen forum is shown to be genuinely inconvenient and the selected forum significantly preferable." Aenergy, S.A., 2022 WL 109945, at \*7. In making this determination, courts consider private and public interest factors. See Iraborri, 274 F.3d at 73. Private interest factors relate to "the convenience of the litigants." Id. They include "the relative ease of access to sources of proof," the ability to obtain witnesses, "and all other practical problems that make trial of a case easy, expeditious and inexpensive." Aenergy, S.A., 2022 WL 109945, at \*7 (citation omitted). Public interest factors include "administrative difficulties associated

with court congestion; the unfairness of imposing jury duty on a community with no relation to the litigation; the interest in having localized controversies decided at home; and avoiding difficult problems in conflict of laws and the application of foreign law.” Id. (citation omitted).

“[A] plaintiff should not [be] deprived of their choice of forum except upon defendants’ clear showing that a trial in the United States would be so oppressive and vexatious to them as to be out of all proportion to plaintiffs’ convenience.” DiRienzo v. Philip Servs. Corp., 294 F.3d 21, 30 (2d Cir. 2002). “[T]he greater the degree of deference to which the plaintiff’s choice of forum is entitled, the stronger a showing of inconvenience the defendant must make to prevail in securing forum non conveniens dismissal.” Iragorri, 274 F.3d at 74.

Because Google’s choice of forum is entitled to significant deference, the defendants must make a strong showing of inconvenience. They have not done so. The defendants assert that litigation in Russia would be more convenient because the defendants are residents of the Russian Federation, and because evidence and witnesses would be located in Russia. But Google is a United States corporation, and evidence may be found in its possession as well. Moreover, the Department of State has

issued a level 4 travel advisory -- its most severe level -- warning against travel to Russia.<sup>5</sup> The defendants have therefore failed to show that litigation in Russia would be more convenient.

The public interest factors also weigh against dismissal. The United States has a significant interest in hearing the litigation, as, allegedly, its citizens have been harmed and its laws broken. See id. at 33. Nor have the defendants identified any material issue of foreign law; each of Google's claims arises under state or federal law. The defendants have therefore failed to present a meritorious forum non conveniens argument.

#### D. Failure to State a Claim

Defendants argue that the default should be vacated and the case dismissed because Google has failed to state a claim upon which relief can be granted. In order to state a claim and survive a motion to dismiss for failure to state a claim, "[t]he complaint must plead 'enough facts to state a claim to relief that is plausible on its face.'" Green v. Dep't of Educ. of

---

<sup>5</sup> See "Russia Travel Advisory", U.S. Dep't of State (Apr. 19, 2022), <https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories/russia-travel-advisory.html>.

City of New York, 16 F.4th 1070, 1076-77 (2d Cir. 2021) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). "In determining if a claim is sufficiently plausible to withstand dismissal," a court "accept[s] all factual allegations as true" and "draw[s] all reasonable inferences in favor of the plaintiffs." Melendez v. City of New York, 16 F.4th 992, 1010 (2d Cir. 2021) (citation omitted).

The defendants argue that Google has failed to state a claim for violations of RICO, the ECPA, and trademark and unfair competition law, for tortious interference with a business relationship, and for unjust enrichment. For the following reasons, however, the defendants' arguments are unavailing. They have presented no meritorious defense that Google's complaint fails to state a claim.

1. RICO

- i. Substantive RICO Violation

To state a claim for a RICO violation, a plaintiff must plausibly allege "(1) a violation of the RICO statute, 18 U.S.C.



§ 1962; (2) an injury to business or property; and (3) that the injury was caused by the violation of Section 1962.” Spool v. World Child Int’l Adoption Agency, 520 F.3d 178, 183 (2d Cir. 2008) (citation omitted). A plaintiff may bring a claim for violation of the RICO statute, and for conspiracy to violate the RICO statute. 18 U.S.C. § 1962(c)–(d). To state a claim for a substantive RICO violation, a plaintiff must allege “a pattern of racketeering activity.” Spool, 520 F.3d at 183 (quoting 18 U.S.C. § 1962(a)–(c)). A pattern of racketeering activity “requires at least two acts of racketeering activity” -- the commission of certain statutorily enumerated crimes -- within “ten years” of each other. 18 U.S.C. § 1961(1), (5).

“A RICO defendant will not be liable for mere participation in a racketeering act.” D’Addario v. D’Addario, 901 F.3d 830, 103 (2d Cir. 2018). The plaintiff must also allege that the defendant participated in the “operation or management of an enterprise through a pattern of racketeering activity.” Id. (quoting Reves v. Ernst & Young, 507 U.S. 170, 184 (1993)). “[T]he ‘operation or management’ test presents a relatively low hurdle for plaintiffs to clear, especially at the pleading stage.” Id. (citation omitted).

The defendants argue that Google has not sufficiently alleged their "operation and management" of any RICO enterprise. But Google's complaint contains detailed allegations of the defendants' criminal schemes to use the Glupteba botnet to steal victims' personal information and sell access to their computers. Additionally, Google has alleged that the defendants each possess email accounts associated with websites that sell the Glupteba Enterprise's services. Finally, Google alleges that the defendants operate the Glupteba botnet's C2 servers, which enable exploitation of the infected computers in the first instance. These allegations are sufficient to plead the defendants' operation and management of the Glupteba Enterprise.

The defendants nevertheless insist that these allegations are insufficient because they do not properly identify the defendants' specific roles in the Glupteba Enterprise's chain of command. But a RICO enterprise does not need to have a "hierarchical structure or a 'chain of command'", and members need not have "fixed roles" within the enterprise. Boyle v. United States, 556 U.S. 938, 948 (2009). Instead, it is sufficient to allege that the enterprise "function as a continuing unit and remain in existence long enough to pursue a course of conduct." Id. Google allegations, detailing an

extended course of unlawful conduct reliant on continuing online infrastructure, are sufficient to satisfy this test.

ii. RICO Conspiracy

Defendants also argue that Google has not sufficiently alleged that they conspired to commit a RICO violation. To state a RICO conspiracy claim, a plaintiff must "allege the existence of an agreement to violate RICO's substantive provisions." Butcher v. Wendt, 975 F.3d 236, 241 (2d Cir. 2020) (citation omitted). A plaintiff can satisfy this requirement by plausibly alleging that "the defendant knew of, and agreed to, the general criminal objective of a jointly undertaken scheme." United States v. White, 7 F.4th 90, 99 (2d Cir. 2021).

Google's complaint plausibly alleges that each of the defendants agreed to commit a RICO violation. Google alleges that the defendants knowingly agreed to commit multiple predicate offenses as part of the Glupteba Enterprise, including wire fraud, identity fraud, and violations of the CFAA. And this allegation is supported by further allegations that the defendants jointly operated multiple websites that formed part of the enterprise, and that they operated the C2 servers controlling the Glupteba botnet. These allegations are sufficient to plausibly plead that the defendants knowingly

agreed not only to the “general criminal objective” of the Glupteba Enterprise, but also many of the specific means by which it would be carried out. See Id.

iii. Extraterritorial application

Finally, the defendants argue that Google has failed to state a RICO claim because RICO does not apply extraterritorially. This argument, however, misconstrues the relevant precedent. A plaintiff may bring a RICO claim arising from foreign activity so long as the plaintiff plausibly alleges “a domestic injury to business or property.” Bascuñán v. Elsaca, 874 F.3d 806, 809 (2d Cir. 2017) (quoting RJR Nabisco, Inc. v. European Cmty., 579 U.S. 325, 346 (2016)). Injuries to property may be domestic for the purposes of RICO even when the property owner does not reside in the United States. Id. at 824. Here, however, Google has alleged a number of domestic injuries to United States residents, including the theft of personal information, and unauthorized access to Google accounts and electronic devices belonging to individuals within the United States. Accordingly, Google’s claim does not seek impermissible extraterritorial application of RICO.

2. ECPA, Trademark, and Unjust Enrichment Claims

The defendants argue that Google has failed to state a claim for unjust enrichment, violation of the ECPA, and violation of trademark and unfair competition law. The defendants do not point to any particular deficiencies in Google's allegations, however, instead insisting that user participation in their online services was voluntary, and that they did not know about or participate in any trademark violations. But Google has pled otherwise, alleging that the defendants operated websites using Google's marks in order to infect user's computers with malware that hijacked their computers and harvested their personal information. When evaluating whether a complaint fails to state a claim, a court must "accept all factual allegations as true." Melendez, 16 F.4th at 1010 (citation omitted). Accordingly, the defendants' disagreement with these allegations does not establish that Google has failed to state an ECPA, unjust enrichment, trademark, or unfair competition claim.

3. Tortious Interference with a Business Relationship

The defendants argue that Google has failed to state a claim for tortious interference with a business relationship. To state a claim for tortious interference with a business

relationship, the plaintiff must plausibly allege that “(1) the plaintiff had business relations with a third party; (2) the defendant interfered with those business relations; (3) the defendant acted for a wrongful purpose or used dishonest, unfair, or improper means; and (4) the defendant’s acts injured the relationship.” 16 Casa Duse, LLC v. Merkin, 791 F.3d 247, 261 (2d Cir. 2015) (citation omitted). A means is “improper” when it “amount[s] to a crime or an independent tort.” Carvel Corp. v. Noonan, 3 N.Y.3d 182, 190 (2004).

Google’s complaint satisfies these requirements. Google has plausibly alleged that it has business relationships with its users, and that the defendants have harmed those relationships by undermining the security of Google’s networks and interfering with users’ accounts.

The defendants argue that Google has not sufficiently alleged that they acted with a wrongful purpose. But a plaintiff can allege that the defendants “acted for a wrongful purpose or used dishonest, unfair, or improper means.” 16 Casa Duse, LLC, 791 F.3d at 261 (emphasis added). Here, Google has alleged that the defendants routinely committed torts and crimes against Google users as part of their scheme, including fraud and violations of the CFAA. These allegations are sufficient to

state a claim for tortious interference with a business relationship, notwithstanding the defendants' disagreement with the allegations as a matter of fact.

### III. Prejudice

A court ruling on a motion to set aside an entry of default must consider "prejudice to the non-defaulting party."

Bricklayers, 779 F.3d at 186. A plaintiff is prejudiced if the defendant's delay "may thwart plaintiff's recovery or remedy, . . . result in the loss of evidence, create increased difficulties of discovery, or provide greater opportunity for fraud and collusion." Green, 420 F.3d at 110 (citation omitted). "Delay alone is not a sufficient basis for establishing prejudice," however, because "some delay is inevitable" when a default is set aside. Id. (citation omitted).

Google argues that setting aside the default could result in the loss of evidence and frustrate Google's efforts to shut down the botnet, because the Glupteba Enterprise has attempted to evade Google's efforts to shut it down, setting up new C2 servers and broadcasting their addresses to infected devices on the blockchain. Google has been issued a preliminary injunction, however, which it may continue to wield against the

Glupteba Enterprise and the individual defendants while the case is ongoing. Additionally, the parties can conduct expeditious and targeted discovery to ensure that they can quickly obtain the evidence they need, without inhibiting Google's efforts to disrupt the Glupteba botnet. Google therefore will not be unduly prejudiced by a grant of the defendants' motion to set aside the entry of default.

#### IV. Doe Defendants

Google requests default judgment against the Doe Defendants, because they have not appeared or responded to the complaint. A default judgment is void if issued against defendants who have not been served. See Rosa v. Allstate Ins. Co., 981 F.2d 669, 679 (2d Cir. 1992). Google has not shown that the Doe Defendants were served, and the Certificate of Default states only that defendants Starovikov and Filippov were served. Accordingly, Google's request for default judgment against the Doe defendants is denied.<sup>6</sup>

---

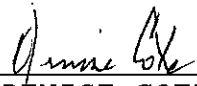
<sup>6</sup> Google cites to other cases involving botnets in which default judgment was entered against Doe defendants. In each of those cases, however, the court found that the Doe defendants had been served. Microsoft Corp. v. Does 1-2, No. 20CV01217, 2021 WL 4260665, at \*2 (E.D.N.Y. Sept. 20, 2021); Microsoft Corp. v. Does 1-51, No. 17CV04556, 2018 WL 3471083, at \*1 (N.D. Ga. June 18, 2018).



**Conclusion**

The defendants' March 14 motion to set aside the entry of default is granted. The defendants' March 14 motion to dismiss is denied. Google's March 25 motion for default judgment is denied.

Dated: New York, New York  
April 27, 2022

  
\_\_\_\_\_  
DENISE COTE  
United States District Judge